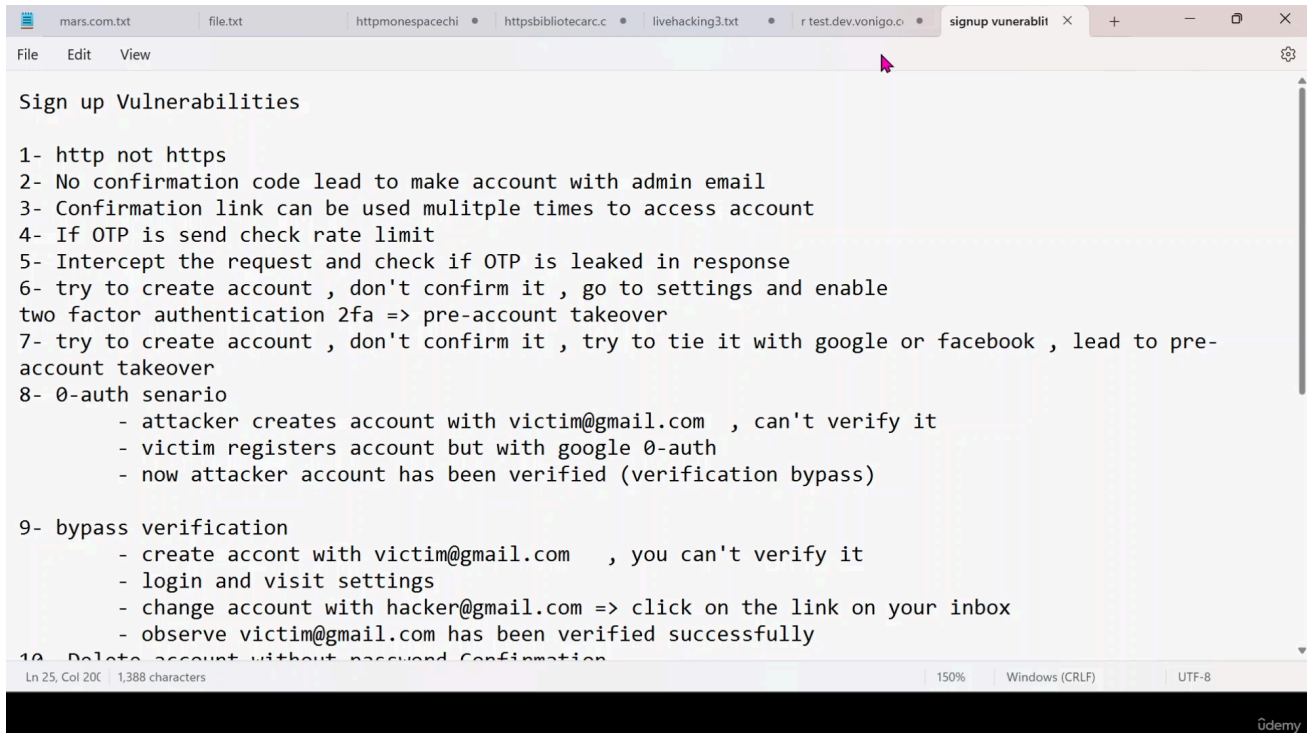


Registration Vulnerabilities

- ثغرات بتبقي ف صفحه ال sign up page



```
Sign up Vulnerabilities

1- http not https
2- No confirmation code lead to make account with admin email
3- Confirmation link can be used multiple times to access account
4- If OTP is send check rate limit
5- Intercept the request and check if OTP is leaked in response
6- try to create account , don't confirm it , go to settings and enable
two factor authentication 2fa => pre-account takeover
7- try to create account , don't confirm it , try to tie it with google or facebook , lead to pre-
account takeover
8- 0-auth senario
  - attacker creates account with victim@gmail.com , can't verify it
  - victim registers account but with google 0-auth
  - now attacker account has been verified (verification bypass)

9- bypass verification
  - create acct with victim@gmail.com , you can't verify it
  - login and visit settings
  - change account with hacker@gmail.com => click on the link on your inbox
  - observe victim@gmail.com has been verified successfully

10- Delete account without password Confirmation
```

- 1 - لو لقيت الموقع شغال http مش https دا Insecure data transfer ودا ممكن تبلغ الثغره عليه
- 2 - لو ملقتش code ببعت علشان ياكدا انت صاحب الاكونت ولا لا ممكن تجرب تعمل اكونت بالـ admin email ولو قديت تعمل اكونت بالشكل دا ممكن تاخد صلاحيات اعلي وتبلغها كثره
- 3 - الـ confirmation link اللي بيوصلك علي gmail علشان ياكدا ايميلك بيستخدم مره واحده بس وبعدھا بيحصله expired لو جيت تفتحه تاني بعد ما استخدمته ولقيت لسه شغال ودخلك علي الاكونت تعتبر ثغره
- 4 - كود التاكيد اللي بيبقي من 6 ارقام بتجرب تتوقعه كذا مره وتشوف هيديك حظر ولا لا لو اتحظرت فدا الطبيعي لو فضل يدك wrong kod ف ممكن تبلغها كثره
- 5 - بتعمل اعتراض لطلب عمل الاكونت وتشوف ف request بتاع ال repeter ممكن تلاقي الكود
- 6 - لو قدرت تعمل اكونت وتخس عليه من غير ماتعمله confirm من الرابط و قدرت تفعل ال 2fa المصادقه الثنائيه ف دي ثغره اسمها pre account takeover
- 7 - لو عملت اكونت برضو ومعلمتش confirm برضو و قدرت تربطو ب فيس او جوجل ف كدا ثغره برضو
- 8 - لو انت حاولت تعمل تسجيل دخول ب الجيميل دا مثلا victim@gmail.com مش هتقدر لان انت مش معاك كود لو حد تاني عمل جيميل بنفس الاسم وسجل دخول ف الموقع من ايقونه جوجل مش هيطلب منو تاكيد وهيخش علطول ف بكدا اكونت انت كمان اتفعل دي ثغره اسمها (Verification bypass)
- 9 - بتعمل اكونت برضو victim@gmail.com ومش هتعرف تفعله وفلما تسجل دخول هيقولك اعمل verify فبتخش علي الاعدادات وتغير الجيميل باميلك انت هيبعتلك confirmation link فلما بتعمله Confirmation الايميل القديم هو اللي بيتأكد بدل الجديد اللي هو بتاعك

```

10- Delete account without password Confirmation |
11- xss via username , name as username=""><u>hossamshady
or      "><svg/onload=confirm(document.cookie)>"@x.y
or      hossam@gmail.com\'"><svg/onload=confirm(1)>
or "><img src=[https://www.no-gods-no-masters.com/images\_designs/anonymous-gandhi-d001001207265.png]
(https://www.no-gods-no-masters.com/images\_designs/anonymous-gandhi-d001001207265.png)\>"@x.y "

```

- 10 - لو جيت تحذف الاكونت ومطلبش منك تطلب الباسورد القديمه دي تعتبر ثغره
- 11 - بتحاول تحقن الاكواد دي الاول بتحقنه ف الاسم تشوف هيحطلك under line تحت الاسم ولا لا والباقي بتجربهم ف الايميل

Sign up Vulnerabilities

- 1- http not https
- 2- No confirmation code lead to make account with admin email
- 3- Confirmation link can be used mulitple times to access account
- 4- If OTP is send check rate limit
- 5- Intercept the request and check if OTP is leaked in response
- 6- try to create account , don't confirm it , go to settings and enable two factor authentication 2fa => pre-account takeover
- 7- try to create account , don't confirm it , try to tie it with google or facebook , lead to pre-account takeover
- 8- 0-auth senario
 - attacker creates account with victim@gmail.com , can't verify it
 - victim registers account but with google 0-auth
 - now attacker account has been verified (verification bypass)
- 9- bypass verification
 - create accont with victim@gmail.com , you can't verify it
 - login and visit settings
 - change account with hacker@gmail.com => click on the link on your inbox
 - observe victim@gmail.com has been verified successfully
- 10- Delete account without password Confirmation
- 11- xss via username , name as username="">[hossamshady](#)
 - or "><svg/onload=confirm(document.cookie)>"@x.y
 - or hossam@gmail.com"><svg/onload=confirm(1)>
 - or ">"@x.y "